Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo Pin	Firewall UTM 3500	1	11/12/2023	MI117

UTM 3500

Nosso firewall é fornecido via contrato através da empresa BluePex; Modelo: UTM 3500;
Versão atual: 6.0.0-REAALEASE; Serial: 86638
O equipamento apresenta as seguintes configurações, vouches, vlans, proxy, webfilter, failover, monitoramento, vpn,.

Regras de firewall: Firewall/Regras/LAN

LAN: Existem atualmente algumas regras que são liberação total, como:
URLSuperBotChat (WhatsApp corporativo); Antivirus_URLs (Antivírus BitDefender); Antivirus_IPs (Antivirus BitDefender); Skype (Links de acesso ao app Skype); fazenda (Links do site da fazenda.gov).
LAN: Liberação de acessos de equipamentos que não necessitam de proxy:
Atualmente temos o acesso dos diretores através da regra de objetos Celulares_foraProxy, Servidores IP cada um com sua regra específica para acesso.
Endereços IPs liberados:
Existe uma regra Temporario, para quando se têm a necessidade temporário de algum endereço de IP para avaliação de acesso a algum determinado serviço. Por padrão sempre fica desativado.
Por Padrão temos uma regra web_portas que bloqueia qualquer acesso de qualquer equipamento que não esteja na lista de IPs liberados e que não tenha Proxy nas estações.

Regas de Firewall: Firewall/Objetos
Nessa categoria é possível criar objetos com vários URLs ou endereços IP que podem ser bloqueados ou liberados em grupo nas regras LAN.

No final da página clique em Adicionar:
Informe os seguintes campos:
Nome:
Descrição:
Tipo: Rede para endereço IP e Host para endereço URL
Informe no campo REDE OU FQDN, caso estiver necessidade pode clicar em + Adicionar Rede.
Após a configuração clique em Salvar.
Com o objeto criado, deverá ir até Firewall/Regras/LAN
Clique no final da página na opção Adicionar, informe os seguintes campos:
Tipo de regra:
Ação: Liberar ou Bloquear
Interface:
Origem: + o nome do grupo do objeto
Clique em Salvar
Depois mova a regra conforme a necessidade, se deverá ser solicitado proxy ou bloqueio total.

WebFilter

WebFilter/Proxy Server
Na opção Servidor iremos definir o servidor proxy do nosso firewall.
Clique em + Adicionar
Informe os seguintes campos:
Nome da Instância: PROXY_SSO
Habilitar: Sim
Interface(s): LAN
Porta do Proxy: 3128
Permitir usuários nas interfaces: Sim
Desabilitar ICMP: Sim
User um servidor DNS alternativo para o servidor proxy: 8.8.8.8
Configurações de autenticação
Metodo de Autenticação: Single SingOn (SSO)
Número de processos de autenticação: 40
Configurações Single SingON (SSO)
Servidor de Autenticação: ServerAD
Nome de usuário SSO: Mesmo do configurado do AD
Senha SSO: Mesmo do configurado do AD
Número de processos de autenticação: 40
IDMAP UID: 10000-20000
Não mantenha as conexões vivas: Sim
Modo SSL: Spliecewhitelist
Interface(s): LAN

Configurações de logs de autenticação
Habilitar Logs: Sim
Hostname visível: localhost
Email de administrador: suporte.ti@sulplast.com.br
Linguagem: Portugues
Modo X-Forwarded Header: Ligado
Tratamento de Caracteres de Espaço em Branco de URI: strip

Clique em Salvar.

WebFilter/Regras

Nosso firewall por padrão tem como bloqueio acesso a internet para todos os usuários, com excesso da seguinte lista conforme aprovação da Diretoria.
Regra DiretoriaGerenteSupervisor, todos que fazem parte desse grupo têm liberação total.
Regra TI, liberação total para os colaboradores de TI.

Regra renata.lopes, a pedido do gestor de RH e autorizado pela Diretoria foi liberado acesso para a funcionário Renata do RH.
Regra Compras, todos os colaboradores do departamento de Compras têm acesso total.
Os demais usuários são bloqueados.
Também existe o bloqueio de Regra por faixa de IP que é separado por departamento, ou seja, mesmo que o usuário tenha acesso de liberação total, porém pode existir alguma lista de endereço de site que é bloqueado para esse endereço IP.

Criando regra de IP e Usuário

Clique no fim da página em + Adicionar
Informe os seguintes campos:
Corresponder: IP, Host ou nome de usuário
Endereço IP ou Nome de Usuário:
Ação: Bloquear todo conteúdo, Permitir todo conteúdo
Lista Customizada: Selecionar as listas que o usuário ou faixa de IP poderá ter acesso ou não
Descrição: Nome Depto ou Usuário
Clique em Salvar

Cirando Listas customizadas

Atualmente existem listas customizadas para cada perfil de acesso, sendo liberado para grupos, usuários ou endereços IPs.
WhatsWeb,LinkedIn,govBrFinanceiro,Bancos,GERAL,Skype,Telefonia,AcessoRemoto,SistemasSulplast,ClientesFornecedores,ServicoSemParar,SiteTreinamentos,Noticias,Saude,Elektro,Teams,ECommerce,OfficeMS,PainelMAV,GeradorSenha,Datamace,SiteTestesMicrofoneA,BloqueioSites,Facebook,Youtube,Instagran,Captive,Wetransfer,PlanosSaude,Zoom,Antivirus,Marketing,Supermercados,Firefox,Estudos,Github,ChatGpt,SuperBotChat,Vimeo
Para criar listas devemos ir até o fim da página, clicar em Adicionar e informar os seguintes campos:
Nome: Nome da lista
URL’s endereço do host adicionando *no começo e/ou no final
Descrição:
Clique em Salvar

VPN

VPN/OpenVPN/Servidores

Para cada tipo de acesso temos VPNs especifica, para acesso de Colaboradores utilizamos a VPN UDP4/1194 Rede de Túneis 172.16.0.0/24
Conceitos utilizamos a VPN UDP4/1195 Rede de Túneis 172.17.0.0/28
Semprel utilizamos a VPN UDP4/1196 Rede de Túneis 172.0.10.0/24

Cada uma com o tipo certo de liberação de acesso.
Cada uma possui seu próprio certificado para conexão e usuário e senha pré-definidos.
Para colaboradores o acesso é feito através de autenticação do AD.
Para criar clique em Adicionar e informar os seguintes campos:
Modo Servidor: Acesso Remoto
Backend para Autenticação:
Protocolo: UDP on IPVA4 only
Modo Dispositivo: turn – Layer 3 Tunnel Mode
Interface:
Porta Local:
Descrição:
Use uma chave TLS: Flegado
Modo de uso de chave TLS: Autenticação de TLS
Direção do keydir TLS: Direction 0
Autoridade de certificação de ponto: CA-SUP
Certificado do Servidor: CERT_SUO (Servidor: sim, CA: CAS-SUP; Em Uso)
DH parâmetro comprimento: 2048 bit
Curva ECDH: Utilizar Padrão
Algoritmo de criptografia: AES-256-CBC (256 bit key, 128 bit block)
Algoritmo de autenticação: SHA256 (256-bit)
Rede de túnel IPV4
Clique em Salvar

VLANs

Interfaces/VLANs

VLAN 10, rede interna; VLAN 15, rede com voucher; VLAN 20, rede de alto acesso.